A new approach to Calculus of Set (Computer Algebra : Design of Algorithms, Implementations and Applications)

AUTHOR(S):

井上, 秀太郎

数理解析研究所講究録
第1652巻 2009年 192-195

A new approach to Calculus of Set

井上 秀太郎
SHUTARO INOUE
東京理科大学大学院理学研究科数学専攻
DEPARTMENT OF MATHEMATICS,GRADUATE SCHOOL OF SCIENCE,TOKYO UNIVERSITY OF SCIENCE*

1 はじめに

$\mathcal{L}$ を定数記号 0,1, 関数記号 $\cap,\cup,^-$, 述語記号 $\subseteq$ を定めた一階述語言語とする. T.Skolem は $\mathcal{L}$ の一階述語論理式が決定可能であることを示した. しかし T.Skolem の限定記号消去の方法は1つ1つの限定記号を段階的に消去するために非常に重い計算となる. 本研究では包括的ブーリアングレブナ基底を使った新しい限定記号消去法を紹介する.

2 ブーリアングレブナ基底

ブーリアングレブナ基底を次のように定義する.

定義 1 全ての要素が冪等であるような、単位元をもつ可換環 B をブール環とよぶ. ブール環 B を係数とする多項式環 $B[X_1,\ldots,X_n]$ のイデアル $\langle X_1^2-X_1,\ldots,X_n^2-X_n\rangle$ による剰余環をブール多項式環とよび、$B(X_1,\ldots,X_n)$ で表す. ブール多項式環におけるグレブナ基底をブーリアングレブナ基底とよぶ.

ブール多項式についての単項式簡約は次のように定義する.

定義 2 ブール多項式 $f=a\alpha+h$ による単項式簡約 $\rightarrow_f$ を

$$b\alpha\beta\rightarrow_f b(1+a)\alpha\beta+ba\beta h$$

と定義する.(ただし $ab\neq 0$ とする.)

体を係数とする多項式環と違う点は、項として簡約できたとしても係数によっては簡約できないことである. 例えば $\{1\}*X*Y$ を $\{2\}*Y+\{1,2\}$ で簡約を試みても $\{1\}(1+\{2\})*X*Y+\{1\}*\{2\}*\{1,2\}*X=\{1\}*X*Y$ となり元の式と変わらない. また簡約が成功したしても必ず次数が下がるとは限らない. 例えば $\{1,2\}*X*Y$ を $\{2\}*Y+\{1,2\}$ で簡約すると $\{1\}*X*Y+\{2\}*X$ となる. 先頭項は共に $X*Y$ となっている. しかし簡約前と簡約後の先頭項が同じ場合でも係数は必ず小さくなる. よって簡約が無限に行われることはない. この現象は係数のブール環が整域ではないために生じる. また多項式 $\{1\}*X+\{2\}$ にたいして定数 $\{2\}$ を掛ける。すると多項式は $\{2\}$ となり先頭項が変化する. このためにブール多項式環では同値関係 $\overset{*}{\leftrightarrow}_F$ とイデアル $\langle F\rangle$ による同値関係は一般に一致しない. これらを解決するために次の用語を導入する.

*j1106701@ed.kagu.tus.ac.jp

定義 3 ブール多項式 f が $lc(f)f = f$ を満たすとき f はブール閉であるという. $lc(f)f$ を f のブール閉包とよび、$bc(f)$ で表す.

以上の定義により与えられた多項式に対して先頭項の係数が 0 になり、先頭項が変化することはなくなる. ブール閉を用いることによってブーリアングレブナ基底の定義に必要な次に定理が成り立つことが示せる.

定理 1 F をブール閉であるブール多項式の集合とする. 同値関係 $\overset{*}{\leftrightarrow}_F$ はイデアル $\langle F\rangle$ による同値関係と一致する. つまり任意のブール多項式 f, g に対して $f \overset{*}{\leftrightarrow}_F g \Leftrightarrow f - g \in \langle F\rangle$ が成り立つ.

以上より先ほどの単項式簡約を用いてブーリアングレブナ基底を定義することができる.

定義 4 多項式の有限集合 G が以下の 2 つの性質を満たすとき、G はブーリアングレブナ基底であるとよぶ.
- 任意のブール多項式 f, g に対して $f \overset{*}{\leftrightarrow}_G g \Leftrightarrow f - g \in \langle G\rangle$ が成り立つ.
- $\rightarrow_G$ がチャーチ・ロッサー性をもつ. つまり任意のブール多項式 f, g, h に対して

$$f \overset{*}{\leftrightarrow}_G g \Leftrightarrow \exists h\ f \overset{*}{\rightarrow}_G h, g \overset{*}{\rightarrow}_G h$$

が成り立つ.

定理 2 G をブール閉である多項式の有限集合とする. このとき G がブーリアングレブナ基底であることは任意の多項式 $f, g \in G$ にたいして $SP(f, g) \overset{*}{\rightarrow}_G 0$ が成り立つことと一致する.

上記の定理はブーリアングレブナ基底の計算も係数が体のときと同じようにできることを示している. 注意しなければならないことは計算途中に現われたブール多項式をブール閉としなければならないことである. また簡約ブーリアングレブナ基底は一意に定まらない. しかし次にような性質を持つ.

定理 3 G を簡約ブーリアングレブナ基底とする. このとき G の任意の要素はブール閉である.

ブーリアングレブナ基底の一意性を得るために次の定義を行う.

定義 5 G を簡約ブーリアングレブナ基底とする. 任意の異なる多項式 $f, g \in G$ にたいして $LT(f) \neq LT(g)$ が成り立つとき G は分層ブーリアングレブナ基底であるとよぶ.

例として 2 つのイデアル $\langle \{1,2\} * X\rangle$ と $\langle \{1\} * X, \{2\} * X\rangle$ を考える. これらは同じイデアルの簡約ブーリアングレブナ基底となっている. しかし前者は分層ブーリアングレブナ基底となるが、後者はならない. このような条件を加えることによりブーリアングレブナ基底の一意性が得られる.

定理 4 G, H は $\langle G\rangle = \langle H\rangle$ を満たす分層ブーリアングレブナ基底であるとする. このとき $G = H$ が成り立つ.

ブール多項式に関しては以下の 2 つの定理が成り立つ.

定理 5 零点定理
I をブール多項式環 $B(\bar{X})$ のイデアルとする. このとき

$$V(I) = \emptyset \Leftrightarrow \exists a \in B \quad a \in I \qquad \text{(弱形の零点定理)}$$

が成り立つ. また I が有限生成であると仮定する. このとき

$$f(\bar{X}) \in I \Leftrightarrow \forall \bar{a} \in V(I)\ f(\bar{a}) = 0 \qquad \text{(強形の零点定理)}$$

が成り立つ.

定理 6 拡張定理
I をブール多項式環 $B(\bar{A},\bar{X})$ のイデアルとする．このとき任意の $\bar{a}\in V(I\cap B(\bar{X}))$ にたいして $(\bar{a},\bar{b})\in V(I)$ となる $\bar{b}$ が存在する．

拡張定理は本研究で重要な役割を果たす．また包括的グレブナ基底を次のように定義する．

定義 6 I を係数が環 R である多項式環 $R[\bar{A},\bar{X}]$ のイデアルとする．このとき有限集合 $G\subseteq I$ が包括的グレブナ基底であるとは、R の拡大環 R' の任意の要素 $\bar{a}$ にたいして、$G(\bar{a})=\{g(\bar{a},\bar{X})|g\in G\}$ が $I(\bar{a})=\{f(\bar{a},\bar{X})|f\in I\}$ のグレブナ基底となることと定義する．

ブール多項式環のイデアルにおける包括的グレブナ基底を包括的ブーリアングレブナ基底と呼ぶ．

3 包括的ブーリアングレブナ基底を使った計算方法

与えられた論理式をブール多項式で表現にするために新しい記号を導入する．述語記号 $sgl(X)$ は集合 X が singlton set であることを意味する．定数記号 $s_1,s_2,\ldots$ は singlton set を表す．また $i\neq j$ ならば $s_i\neq s_j$ とする．定数記号 $a_1,a_2,\ldots$ は singlton set の要素を表す．以上の記号を使えば $s_2\cup s_5=\{a_2,a_5\}$ と表すことができる．

要素に関係する限定記号として $\exists_1$ と $\forall_1$ を使用する．$\exists_1 xP(\{x\})$ と $\forall_1 Q(\{x\})$ はそれぞれ $\exists X(sgl(X)\wedge P(X))$ と $\forall X(sgl(X)\rightarrow Q(X))$ を意味する．また記号 $\in$ を使用する．$x\in A$ は $\{x\}\cap A=\{x\}$ を表す．$A\neq B$ は $A+B\neq 0$ と等しい．よって $\exists_1 x(x\in A+B)$ と表すことができる．

これらの記号を使用して，与えられた論理式から存在記号の消去を行う．次のような論理式を与える．

$$\exists_1 z_1\ldots\exists_1 z_l\exists Y_1\ldots\exists Y_m\Phi(\{z_1\}\ldots\{z_l\},Y_1,\ldots Y_m,X_1\ldots,X_n)$$

始めにこの論理式を次のような形に変換する．ここで f_i はブール多項式とする．

$$\exists_1 z_1\ldots\exists_1 z_l\exists Y_1\ldots\exists Y_m(\wedge_{i=1}^{k} f_i(\{z_1\}\ldots\{z_l\},Y_1,\ldots Y_m,X_1\ldots,X_n)=0)$$

次に $\{z_1\}\ldots\{z_l\}$ を $A_1\ldots A_l$ に置き換える．そして $Y_1,\ldots Y_m,X_1\ldots,X_n$ を変数，$A_1\ldots A_l$ をパラメータとし，ブロックオーダー $Y_1,\ldots Y_m\gg X_1\ldots,X_n$ でのイデアル $\langle f_1\ldots f_k\rangle$ の包括的ブーリアングレブナ基底を計算する．このグレブナ基底は一般的に次のような形になる．

$$\begin{aligned}
&p_1(Y_1,\ldots Y_m,X_1\ldots,X_n,A_1\ldots A_l),\\
&\vdots\\
&p_r(Y_1,\ldots Y_m,X_1\ldots,X_n,A_1\ldots A_l),\\
&g_1(X_1\ldots,X_n,A_1\ldots A_l),\\
&\vdots\\
&g_s(X_1\ldots,X_n,A_1\ldots A_l),\\
&h_1(A_1\ldots A_l),\\
&\vdots\\
&h_t(A_1\ldots A_l)
\end{aligned}$$

拡張定理から 2 つの論理式

$$\exists_1 z_1 \ldots \exists_1 z_l \exists Y_1 \ldots \exists Y_m (p_1 = 0 \wedge \ldots \wedge p_r = 0 \wedge g_1 = 0 \wedge \ldots \wedge g_s = 0 \wedge h_1 = 0 \wedge \ldots \wedge h_t = 0)$$

と

$$\exists_1 z_1 \ldots \exists_1 z_l (g_1 = 0 \wedge \ldots \wedge g_s = 0 \wedge h_1 = 0 \wedge \ldots \wedge h_t = 0)$$

は等しい. さらに拡張定理を適用することで次の論理式を得る.

$$\exists_1 z_1 \ldots \exists_1 z_l (h_1(\{z_1\}, \ldots, \{z_l\}) = 0 \wedge \ldots \wedge h_t(\{z_1\}, \ldots, \{z_l\}) = 0)$$

このとき $h_1(\{a_{n_1}\}, \ldots, \{a_{n_l}\}) = 0, \ldots, h_t(\{a_{n_1}\}, \ldots, \{a_{n_l}\}) = 0$ を満たす $a_{n_1}, \ldots, a_{n_l}$ に対して,

$$\{g_1(X_1 \ldots, X_n, \{a_{n_1}\}, \ldots, \{a_{n_l}), \ldots, g_s(X_1 \ldots, X_n, \{a_{n_1}\}, \ldots, \{a_{n_l})\}$$

はブーリアングレブナ基底になる. よって $g_1 = 0 \wedge \ldots \wedge g_s = 0 \wedge h_1 = 0 \wedge \ldots \wedge h_t = 0$ は論理式

$$\exists_1 z_1 \ldots \exists_1 z_l \exists Y_1 \ldots \exists Y_m (\wedge_{i=1}^{k} f_i(\{z_1\} \ldots \{z_l\}, Y_1, \ldots Y_m, X_1 \ldots, X_n) = 0)$$

の解をパラメータを使って表している. これはグレブナ基底を使うことで得られる特徴の 1 つである.

4 まとめ

包括的ブーリアングレブナ基底を使用することで, 限定記号消去の高速計算が可能になった. しかし本研究で成功しているのは存在記号の消去だけである. 今後は全称記号を含む論理式や. 集合の濃度に関する論理式も扱えるようにしていきたい.

参 考 文 献

[1] Suzuki, A. and Sato, Y.(2003).An Alternative approach to Comprehensive Gröbner Bases. J. Symb. Comp. 36/3-4,649-667.

[2] Weispfenning, V.(1989).Gröbner bases in polynomial ideals over commutative regular rings, EUROCAL'87,J.H.Davenport Ed.,Springer LNCS 378,336-347.

[3] Weispfenning, V.(1992).Comprehensive Gröbner Bases, J. Symb. Comp.14/1,1-29.